



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,834	03/26/2004	Blayn W. Beenau	60655.9700	2833
20322	7590	05/25/2006		
SNELL & WILMER ONE ARIZONA CENTER 400 EAST VAN BUREN PHOENIX, AZ 85004-2202			EXAMINER NGUYEN, NAM V	
			ART UNIT 2612	PAPER NUMBER

DATE MAILED: 05/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

8

**Office Action Summary**

Application No.

10/708,834

Applicant(s)

BEENAU ET AL.

Examiner

Nam V. Nguyen

Art Unit

2612

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --****Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 4/20/06.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-53 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-53 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

This communication is in response to applicant's Amendment which is filed April 20, 2006.

An amendment to the claims 1, 3, 7-8, 10, 12, 16, 20-23, 25-28, 31-36, 38-40 and 42-46 has been entered and made of record in the application of Beenau et al. for a "method and system for keystroke scan recognition biometrics on a fob" filed March 26, 2004.

The new set of claims 47-53 are introduced.

Claims 1-53 are pending.

### ***Response to Arguments***

Based upon the applicants submitted a terminal disclaimer, in compliance with 37 C.F.R. § 1.321 (c), therefore the examiner has withdrawn double patenting rejections.

In view of applicant's amendment to amend the Claims 1, 3, 7-8, 10, 12, 16, 20-23, 25-28, 31-36, 38-40 and 42-46 to obviate the §112 rejections, therefore, examiner has withdrawn the rejection under 35 U.S.C §112, second paragraph.

Applicant's amendment and arguments with respect to claims 1-46, filed April 20, 2006 have been fully considered but are moot in view of the new ground(s) of rejection.

***Claim Objections***

Claim 49 is objected to because of the following informalities: Claim 49 recites the limitation "wherein said first user account and said second user account" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-47, 49-50 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kita (US# 6,703,918) in view of Bolle et al. (US# 6,819,219) and in view of Griswold et al. (US# 6,629,591).

Referring to claims 1, 22 and 34, Kita discloses a method and a transponder-reader transaction system (i.e. an authentication system) (see Figures 3, 10-11, 14-15, 20 and 24-25) configured with a biometric security apparatus (1) (i.e. a portable information equipment), said system comprising:

a transponder (171) (i.e. a portable information equipment) configured to communicate with a reader (191) (i.e. authentication device) (column 10 line 63 to column 12 line 67; see

Art Unit: 2612

Figure 10-11); a reader (191) (i.e. authentication device) configured to communicate with said system (197) (i.e. system or server) (column 12 line 6 to 67; see Figure 11); a biometric sensor (8 or 10) configured to detect a proffered biometric scan sample (i.e. authentication data), said biometric scan sensor (8 or 10) configured to communicate with said system (197) (i.e. system or server); and a device (152) (i.e. a control circuit) configured to verify said proffered biometric scan sample (i.e. authentication data) to facilitate a transaction (column 19 line 48 o 67; see Figures 24-25).

However, Kita did not explicitly disclose a keystroke scan sensor configure to detect a proffered keystroke scan sample and said device further configured to verify whether said proffered keystroke scan sample is associated with a preset transaction limitation independent of a financial account transaction limitation.

In the same field of endeavor of biometric identity verification system, Bolle et al. teach that a keystroke scan sensor (904) (i.e. a keystroke pattern) configure to detect a proffered keystroke scan sample (i.e. keystroke pattern properties) (column 7 lines 14 to 26; see Figures 1-11) in order to identify the identity of a person using the biometric means for access control.

One of ordinary skilled in the art recognizes using keystroke patterns in a wireless portable communications device taught by Bolle et al. in a portable information equipment of Kita because Kita suggests it is desired to provide that the portable information equipment includes plurality of biometric sensors to authenticate the user (column 10 line 62 to column 12 line 40; column 14 lines 42 to 61; see Figures 10-15) and Bolle et al. teach that the wireless portable communication device includes a plurality of biometric sensors including a keystroke patterns to identify the user in the identity verification system in order to increase security for

Art Unit: 2612

access control. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to using a keystroke patterns in a wireless portable communications device taught by Bolle et al. in a portable information equipment of Kita with the motivation for doing so would have been to secure the verification of the user in the identity verification system for e-commerce.

In the same field of endeavor of portable electronic device, Griswold et al. teach that determining whether said biometric sample (i.e. biometric information of user) is associated with a preset transaction limitation (column 9 lines 30 to 55; see Figure 5) in order to authorize to proceed with the requested transaction.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using biometric information associated with a predetermined preset transaction limit taught by Griswold et al. in a portable information equipment authentication device of Kita in view of Bolle et al. because verifying a biometric information associated with a preset transaction limits would improve security of using a portable electronic device and to minimize time spent accessing a user accounts.

Referring to Claims 2 and 35, Kita in view of Bolle et al. and Griswold et al. disclose the method and the transponder-reader transaction system of claims 1 and 34, Kita discloses wherein said sensor (155) (i.e. organic measurement sensor) is configured to communicate with said system (197) via at least one of a transponder (171) (column 12 line 6 to 40; see Figures 10-15)

Referring to Claims 3 and 38, Kita in view of Bolle et al. and Griswold et al. disclose the method and the transponder-reader transaction system of claims 1 and 34, Kita discloses wherein said keystroke scan sensor (176) is configured to facilitate a limited number of scans (column 4 line 20 to column 5 line 9; column 10 line 62 to column 11 line 61; see Figures 1-3 and 10-15).

Referring to Claims 4 and 39, Kita in view of Bolle et al. and Griswold et al. disclose the method and the transponder-reader transaction system of claims 1 and 34, Kita discloses wherein said keystroke scan sensor (176) is configured to log at least one of a detected keystroke scan sample, processed keystroke scan sample and stored keystroke scan sample (column 5 lines 55 to column 6 line 43; column 9 line 66 to column 10 line 13).

Referring to Claim 5, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses further including a database (154) (i.e. organic authentication registration data) configured to store at least one data packet (i.e. authentication data), wherein said data packet (i.e. authentication data) includes at least one of proffered and registered keystroke scan samples, proffered and registered user information, terrorist information, and criminal information (column 10 line 62 to column 11 line 14; column 12 line 6 to 67; see Figures 10-15).

Referring to Claim 6, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 5, Kita discloses wherein said database (154) (i.e. organic authentication registration data) is contained in at least one of the transponder (151),

Art Unit: 2612

transponder reader, sensor, remote server, merchant server and transponder-reader system (column 10 line 62 to column 11 line 14; column 12 line 6 to 67; see Figures 10-15).

Referring to Claim 7, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 5, Kita discloses wherein said remote database (154) (i.e. organic authentication registration data) is configured to be operated by an authorized sample receiver (356) (i.e. a radio transmission/reception) (column 10 line 62 to column 11 line 14; column 16 lines 42 to column 17 line 39; see Figures 10-15 and 20).

Referring to Claims 8 and 36, Kita in view of Bolle et al. and Griswold et al. disclose the method and the transponder-reader transaction system of claims 1 and 34, Bolle et al. disclose wherein said keystroke scan sensor device (904) (i.e. keystroke pattern) is configured with at least one of electronic sensor (column 6 lines 15 to 42; column 7 lines 14 to 26; see Figures 6 to 11).

Referring to Claims 9, 30 and 43, Kita in view of Bolle et al. and Griswold et al. disclose the method and the transponder-reader transaction system of claims 1, 28 and 34, Bolle et al. disclose wherein said keystroke scan sensor (904) is configured to detect and verify keystroke scan characteristics including at least one behavioral, temporal and physical characteristics (column 7 lines 14 to 26; see Figures 6 to 11).



Art Unit: 2612

Referring to claims 10, 31, and 41, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claims 1, 22, and 34, Bolle et al. discloses wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system further comprises using said keystroke scan sensor (904) to detect false keystrokes and body heat (column 6 lines 15 to 42; column 7 lines 14 to 58; see Figures 6 to 11).

Referring to Claims 11, 42 and 44, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claims 1 and 34, Kita discloses further including a device (152) (i.e. a control circuit) configured to compare a proffered keystroke scan sample (i.e. organic data input) with a stored keystroke scan sample (178) (i.e. registered biometric data) (column 12 lines 6 to 67; see Figure 15).

Referring to claims 12 and 46, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claims 11 and 34, Griswold et al. disclose wherein said stored biometric sample is stored by at least one of a third-party biometric security vendor (112) (i.e. a processing station) (column 8 lines 55 to column 9 line 8; see Figure 4).

Referring to Claim 13, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 11, Kita discloses wherein a stored keystroke scan sample comprises a registered keystroke scan sample (column 12 lines 6 to 67; see Figure 15).

Art Unit: 2612

Referring to Claim 14, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 13, Kita discloses wherein said registered keystroke scan sample (178) (i.e. registered biometric data) is associated with at least one of: personal information, credit card information, debit card information, savings account information, and loyalty point information (column 19 line 47 to 67; see Figure 25).

Referring to Claim 15, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 14, Kita discloses wherein different registered keystroke scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, and loyalty point information (column 19 line 47 to 67; see Figure 25).

Referring to Claims 16 and 49, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 14, Kita discloses wherein a keystroke scan sample (i.e. authentication data) is primarily associated with at least one of first user information (i.e. first authentication registration input) wherein said first information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, and wherein a keystroke scan sample is secondarily associated with at least one of second user information (i.e. first authentication registration input), wherein said second information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, where second user

Art Unit: 2612

information is different than first user information (column 9 line 49 to column 10 line 13; column 19 line 48 to 67; see Figures 9 and 25).

Referring to Claim 17, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said transponder-reader transaction system is configured to begin mutual authentication upon verification of said proffered keystroke scan sample (column 16 lines 47 to column 17 line 25; see Figure 25).

Referring to Claim 18, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said transponder is configured to deactivate (i.e. end the process of verification) upon rejection (i.e. not coincident) of said proffered keystroke scan sample (column 7 line 53 to column 8 line 23; see Figures 6-8).

Referring to Claim 19, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said sensor is configured to provide a notification upon detection of a sample (column 5 line 40 to column 6 line 23; see Figure 5).

Referring to Claim 20, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction (column 19 line 48 to 67; see Figure 25).

Referring to Claim 21, Kita in view of Bolle et al. and Griswold et al. disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure (column 19 line 48 to 67; see Figure 25).

Referring to claim 23, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22, Kita discloses further comprising registering at least one keystroke scan sample (i.e. authentication data) with an authorized sample receiver (8) (column 9 line 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 24, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 23, Kita discloses wherein said step of registering further includes at least one of: contacting said authorized sample receiver (32) (i.e. a wireless transmission reception section), proffering a keystroke scan to said authorized sample receiver (32), processing said keystroke scan to obtain a keystroke scan sample (i.e. authentication data), associating said keystroke scan sample (i.e. authentication data) with user information, verifying said keystroke scan sample (i.e. authentication data), and storing said keystroke scan sample upon verification (column 9 lines 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 25, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22, Bolle et al. discloses wherein said step of proffering includes proffering a

Art Unit: 2612

keystroke scan to at least one of an electronic sensor, an optical sensor and a keyboard (column 6 lines 15 to 42; column 7 lines 14 to 26; see Figures 6 to 11).

Referring to claims 26 and 37, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claims 22 and 34, Kita discloses wherein said step of proffering further includes proffering a biometric (i.e. fingerprint) to a biometric sensor (8) communicating with said system to initiate at least one of: storing, comparing, and verifying said biometric sample (i.e. authentication data) (column 9 lines 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 27, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22, Kita discloses wherein said step of proffering a keystroke scan to a keystroke scan sensor (8) communicating with said system to initiate verification further includes processing database information (i.e. authorized data in an organic authentication registration data), wherein said database information (registration data) is contained in at least one of a transponder (151) (i.e. a equipment) (column 10 line 63 to column 11 line 61; see Figures 10-11).

Referring to claim 28, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22, Kita discloses wherein said step of proffering a keystroke scan to a keystroke scan sensor (8) communicating with said system to initiate verification further includes comparing a proffered biometric sample (i.e. authentication data) with a stored biometric sample

Art Unit: 2612

(i.e. organic authentication registration data registered in the organic authentication registration data unit 154) (column 11 line 42 to 61; see Figures 10-11).

Referring to claim 29, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 28, Kita discloses wherein said step of comparing includes comparing a proffered biometric sample (i.e. authentication data) to a stored biometric sample (i.e. registration data) by using at least one of a third-party security vendor device (37) (i.e. service business) and protocol/sequence controller ((152) (i.e. a control circuit) (column 5 line 40 to column 7 line 52; column 10 line 62 to column 11 line 67; see Figure 1-7 and 10-11).

Referring to claims 32 and 42, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22 and 34, Kita discloses wherein said step of proffering a biometric to a biometric sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered biometric sample (i.e. authentication data) (column 9 line 66 to column 10 line 36).

Referring to claim 33, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 22, Kita discloses wherein said step of proffering a biometric to a biometric sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure (i.e. second authentication input section) (column 10 line 50 to 60; column 11 line 42 to column 12 line 4; see Figures 9-11).

Referring to claim 45, Kita in view of Bolle et al. and Griswold et al. disclose the method for of claim 34, Kita discloses wherein said step of verifying includes verifying a proffered biometric sample using information contained on at least one of a local database (i.e. an organic authentication registration data at the equipment 154) (column 11 line 42 to 61; see Figure 10).

Referring to claims 47, 50 and 52, Kita in view of Bolle et al. and Griswold et al. disclose method of claim 1, Griswold et al. disclose wherein said preset transaction limitation comprises at least one of a maximum transaction amount (i.e. a credits limit) (column 10 lines 9 to 22).

Claims 48, 51 and 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kita (US# 6,703,918) in view of Bolle et al. (US# 6,819,219) and in view of Griswold et al. (US# 6,629,591) as applied to Claims 1, 22 and 34 above, and in further view of Prorock et al. (PUB NO: 2002/0169673 A1).

Referring to Claims 48, 51 and 53, Kita in view of Bolle et al. and Griswold et al. disclose method of Claims 1, 22 and 34, however, Kita in view of Bolle et al. and Griswold et al. did not explicitly disclose further comprising requiring a second proffered biometric sample to override said preset transaction limitation.

In the same field of endeavor of a biometric device for security transaction system, Prorock et al. teach that a second proffered biometric sample (i.e. a manager's fingerprint) to override said preset transaction limitation (i.e. user defined limits) (page 1 paragraph 0002) in order avoid using a physical key and a keying sequence to perform the override procedure.

Art Unit: 2612

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using biometric information of a manager to override a predetermined preset transaction limit taught by Prorock et al. in a portable information equipment authentication device of Kita in view of Bolle et al. and Griswold et al. because verifying a biometric information of a manager to override a preset transaction limits would improve security and increase efficiently of using a portable electronic device in a general transaction system.

### *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.




Houvener (US# 6,424,249) discloses a positive identity verification system and method including biometric user authentication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 571-272-3061. The examiner can normally be reached on Mon-Fri, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wendy Garber can be reached on 571- 272-7308. The fax phone numbers for the organization where this application or proceeding is assigned are 571-273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nam Nguyen  
May 22, 2006



BRIAN ZIMMERMAN  
PRIMARY EXAMINER